Technical Safety Requirements

Development Procedure

February 2003

University of California
Lawrence Livermore
National Laboratory

This page intentionally left blank.

TABLE OF CONTENTS

ACRONYMS

AA	Accident Analysis
AC	Administrative Control
ANSI	American National Standard Institute
AOT	Allowable Outage Time
CFR	Code of Federal Regulations
CIS	Control Item Selection
CN	Change Notice
DBA	Design Basis Accident
DF	Design Feature
DID	Defense-in-depth
DOE	Department of Energy
DOT	Department of Transportation
DSA	Documented Safety Analysis
EG	Evaluation Guideline
ERPG	Emergency Response Planning Guideline
ES&H	Environmental, Safety, and Health
HA	Hazard Analysis
HVAC	Heating, Ventilating, and Air-conditioning
IC	Initial Condition
LCO	Limiting Condition for Operation
LCS	Limiting Control Setting
LLNL	Lawrence Livermore National Laboratory
NFPA	National Fire Protection Association
OSHA	Occupational Safety and Health Administration
QA	Quality Assurance
SAR	Safety Analysis Report
SC	Safety Class
SIH	Standard Industrial Hazard
SL	Safety Limit
SR	Surveillance Requirement
SS	Safety Significant
SSC	Structures, Systems, and Component
STD	Standard
TSR	Technical Safety Requirement

This page intentionally left blank.

1. PURPOSE

This procedure provides the requirements, responsibilities, and methodology for preparing Technical Safety Requirements (TSRs) for Lawrence Livermore National Laboratory (LLNL) Nuclear Hazard Category 2 and 3 Facilities. It provides direction in the development of Safety Limits, Limiting Control Settings, Limiting Condition for Operations, Administrative Controls, and Design Features, consistent with the information contained in a given Documented Safety Analysis (DSA).

This page intentionally left blank.

2. SCOPE

The scope of this procedure is consistent with the Control Item Selection (CIS) guidance provided in Department of Energy Standard (DOE-STD) 3009-94, Change Notice (CN) 1 (Ref. 1). This procedure applies to any LLNL CIS task initiated or revised after this procedure becomes effective and performed in accordance with either of the following safe harbor methods of Title 10, Code of Federal Regulations, Part 830 (10 CFR 830) (Ref. 2):

- DOE-STD-3011-94 (Ref. 3).
- DOE-STD-3009-94.

The methodology presented in this procedure meets the requirements of 10 CFR 830 and the *LLNL Safety Basis Program Plan for Category 2 and 3 Nuclear Facilities* (AB-001) (Ref. 4). Deviations from this procedure require the approval of the Authorization Basis Section Leader. Subcontractors may follow their own procedure, provided it meets the requirements of DOE-STD-3009-94 and that documentation of the procedure is provided to the Authorization Basis Section Leader and Nuclear Facility Associate Director for acceptance prior to beginning the process.

10 CFR 830 allows nuclear facilities that either have a limited operational life or are subject to deactivation to make use of the alternate safe harbor methodology in DOE-STD-3011-94. The categories of controls designated and associated documentation specified in DOE-STD-3011-94 may vary from that in DOE-STD-3009-94. To the extent that this applies, the TSR development methodology of this procedure may be used as conceptual guidance.

This procedure does not cover performing or documenting CIS. The CIS process used to implement this procedure must be conducted in accordance with the LLNL Control Item Selection (CIS) Procedure (AB-007) (Ref. 5).

TSR development is an end result of the hazard analysis, accident analysis, and CIS process documented in a DSA. The CIS process identifies Safety Class (SC) and Safety Significant (SS) Structures, Systems, and Components (SSCs) as well as significant non-SSC (i.e., administrative) controls. The CIS process also identifies those initial conditions and major assumptions from the Hazard Analysis (HA) and Accident Analysis (AA) that the TSRs must protect. The TSR development process turns this input into a formally defined TSR document, both in terms of specific controls [e.g., developing the LCO Statements, Mode Applicability, Actions, Surveillance Requirements (SR) and the associated Bases sections] and the framework (e.g., developing the modes of operation, definitions, general rules of applicability) within which those controls are implemented.

2.1 INPUTS

Input to the TSR development process should include the following:

- Facility description, including process and activity descriptions (DSA Chapter 2).
- Hazard analysis tables.

- Hazard analysis discussion of events with significant potential for uncontrolled release of radioactive or other hazardous material or energy and the controls available to prevent or mitigate such events (DSA Section 3.3.2.3.2).
- Hazard analysis discussion of the events identified as presenting a significant hazard to workers and the controls available to prevent or mitigate such events (DSA Section 3. 3.2.3.3).
- Accident analysis information of the events that challenge offsite evaluation guidelines and the controls available to prevent or mitigate such events (DSA Section 3.4).
- Any additional control item selection documentation deemed relevant.

2.2 OUTPUTS

The primary output of the TSR development process is the TSR document developed for a specific facility, including:

- Specification of the TSR controls by type (e.g., safety limit, limiting control setting, limiting condition for operation, administrative control, and design feature).
- Preparation of the required definitional framework (e.g., modes, definitions, and general rules of applicability).
- Preparation of each type of TSR control identified (e.g., preparing LCO Statement, Modes Applicability, Process Area Applicability, Surveillance Requirements and Actions, the Bases section, Administrative Controls, and Design Features).

3. TERMS AND DEFINITIONS

Accident – An unplanned sequence of events that results in undesirable consequences.

Accident Analysis (AA) – Those bounding analyses selected for inclusion in the Documented Safety Analysis (DSA). Historically, AA has consisted of formally developing numerical estimates of the expected consequences and probability of potential accidents associated with a facility. An AA is a follow-on effort to the HA, not a fundamentally new examination requiring extensive original work. As such, it requires documenting the basis to assign a given likelihood of occurrence range in the HA and performing a formally documented consequence analysis. Consequences are compared with offsite EGs to identify Safety Class SSCs.

Administrative Controls – Provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility.

Bases appendix – An appendix that describes the basis of the limits and other requirements in TSRs.

Consequence – The result or effect of a release of hazardous material (radiological, chemical, or biological).

Defense-in-Depth (DID) – The DID philosophy is a fundamental approach to hazard control in which no one layer of protection, by itself, no matter how good, is solely relied upon. To compensate for potential human and mechanical failures, DID is based on several layers of protection with successive barriers to prevent or mitigate the release of hazardous material to the environment. In keeping with the graded-approach concept, demonstrating a generic, minimum number of DID layers is not required. However, defining DID as it exists at a given facility is crucial for determining a safety basis. (For a more detailed definition of DID, see DOE-STD-3009-94.)

Design Features – The design features of a nuclear facility specified in the Technical Safety Requirements that, if altered or modified, would have a significant effect on safe operation.

Documented Safety Analysis – A documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety.

Equipment important to safety – For the purposes of this procedure, equipment important to safety includes any equipment whose function can affect safety either directly or indirectly as described in the safety basis. This includes safety class and safety significant SSCs, and other systems that perform an important DID function; equipment relied on for safe shutdown; and in some cases, process equipment. These considerations apply to both workers and the public. [This definition is taken from DOE guidance on the Unreviewed Safety Question (USQ) process.]

Evaluation Guideline (EG) – The offsite public radiological dose against which the safety analysis is evaluated for safety class determination. (NOTE: LLNL has also specified a LLNL-specific chemical EG for safety significant designation.)

Event – An unplanned occurrence, sequence of occurrences, or phenomena that may result in a release of radiological or chemical hazardous material or energy.

Hazard – A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel; damage to a facility; or damage to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).

Hazard Analysis (HA) – A comprehensive assessment of facility hazards and associated accident scenarios that could produce undesirable consequences for the onsite population, the public, or the environment. Hazard identification and hazard evaluation are included.

Hazard Evaluation – A hazard analysis step that evaluates the significance of hazardous situations associated with a process or activity. Hazard evaluations prepared in compliance with the LLNL Hazard Analysis Procedure (AB-004) include both unmitigated and mitigated evaluations, defined as follows:

> **Unmitigated Evaluation** – Estimates the risks involved with a facility and its associated operations without regard for safety controls or programs. "Unmitigated" refers to estimating frequency and consequences without taking into account preventive or mitigative features other than initial conditions and a given operation's basic physical realities.
>
> **Mitigated Evaluation** – Estimates the risks involved with a facility and its associated operations presuming the availability of safety controls and programs.

Initial Conditions (ICs) – Specific assumptions regarding a facility and its operations included in an unmitigated evaluation. ICs generally are intended to facilitate scenario definition and include items such as inventory information and capabilities of passive features (i.e., no mechanical or human involvement).

Limiting Conditions for Operation – The limits that represent the lowest functional capability or performance level of safety structures, systems, and components required for safe operations.

Limiting Control Settings – The settings on safety systems that control process variables to prevent exceeding a safety limit.

Nuclear Facility – A reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of DOE that includes any related area, structure, facility, or activity to the extent necessary to ensure proper implementation of the requirements established by 10 CFR 830.

Nuclear Facility Associate Director – The Associate Director assigned to a given nuclear facility for which a DSA and TSRs are being prepared.

Offsite Public – All individuals outside of the DOE site boundary. For LLNL Site 200, this boundary is defined by the perimeter fence line. Upon closure of East Avenue, it will expand southward to encompass East Avenue to its control points and the adjacent Sandia DOE site.

Operating Limits – Those limits required to ensure the safe operation of a nuclear facility, including limiting control settings and conditions for operation.

Safety Basis – The DSA and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely to adequately protect workers, the public, and the environment.

Safety Class Function - A preventive or mitigative function that must be performed to keep radiological exposure to the offsite public from challenging the radiological evaluation guideline.

Safety Class SSC – An SSC that performs a safety class function.

Safety SSCs - The set of SC and SS SSCs for a given facility.

Safety Significant Function – A preventive or mitigative function whose performance is a major contributor to DID (i.e., prevention of uncontrolled material releases) or worker safety, as determined from the hazard analysis, or which keeps chemical exposure to the offsite public below the LLNL-specific chemical evaluation guideline.

Safety Significant SSCs – An SSC that performs a safety significant function.

Standard Industrial Hazards – Hazard sources (material or energy) routinely encountered by the general public, or in general industry and construction for which national consensus codes or standards exist to govern handling or use without special analysis to define safety design or operational parameters.

Surveillance Requirements – Requirements relating to test, calibration, or inspection to ensure: 1) maintenance of the necessary operability and quality of safety SSCs and their support systems required for safe operations, 2) that facility operation is within safety limits, and 3) that control setting limits and condition limits for operation are met.

Technical Safety Requirements – The limits, controls, and related actions that establish the specific parameters and requisite actions for the safe operation of a nuclear facility and include, as appropriate for the work and hazards identified in the documented safety analysis for the facility: safety limits, operating limits, surveillance requirements, administrative and management controls, use and application provisions, and design features, as well as a bases appendix.

Use and Application Provisions – The basic instructions for applying Technical Safety Requirements.

Workers – Individuals either immediately adjacent to or within the occupied area of hazard, or outside the occupied area of hazard but within the site boundary. This latter group is sometimes referred to as co-located workers. In accident analysis, doses are sometimes reported for a generic co-located worker 100 meters from the facility in question.

This page intentionally left blank.

4. RESPONSIBILITIES

TSR development is an end result of the DSA process. Responsibilities for TSR development are linked to responsibilities for developing the DSA. The individual who executes each specific responsibility depends on the facility involved and the level of staffing associated with the TSR development process. This section specifies responsibilities for the various aspects of the TSR development process

4.1 FACILITY MANAGER

The facility manager is responsible for:

- Authorizing preparation of a DSA
- Designating the DSA leader
- Determining the funding and schedule for DSA and TSR development
- Identifying the staff to provide facility-specific input to the TSR development process
- Resolving issues and questions regarding facility operations, facility engineering, and regulatory matters
- Ensuring that the TSR process documentation and approval are consistent with applicable Quality Assurance (QA) requirements
- Approving the DSA and the TSR document

4.2 DOCUMENTED SAFETY ANALYSIS LEADER

The DSA leader is responsible for:

- Ensuring that the DSA is developed on schedule and within budget
- Interfacing with facility personnel to ensure that facility-specific inputs to the TSR are accurate and consistent with other DSA input
- Working to resolve issues and questions related to the DSA and TSR
- Raising issues and questions to the facility manager for resolution
- Ensuring that the output of the TSR development process is documented and submitted to the facility manager consistent with applicable QA requirements.
- Ensuring that the TSR development process involves qualified staff and appropriate expertise

4.3 DOCUMENTED SAFETY ANALYSIS TEAM

DSA team members (e.g., operations, criticality safety, structural) are responsible for:

- Interacting with facility staff and others to ensure appropriate input to the TSR.
- Performing their work in accordance with the DSA and other relevant procedures.
- Working to resolve issues associated with the TSR.
- Informing the DSA leader of issues associated with TSR development that may affect the DSA's conclusions, budget, or schedule.
- Preparing, documenting, and submitting the TSR document consistent with applicable QA requirements.

4.4 ENVIRONMENTAL SAFETY AND HEALTH TEAM

The ES&H Team assigned to the facility is responsible for (as applicable and when requested):

- Providing input to the TSR development process.
- Providing staff with expertise to assist the TSR development process.
- Reviewing the TSR document.

4.5 AUTHORIZATION BASIS SECTION LEADER

The authorization basis section leader is responsible for:

- Approving any deviations from this procedure.
- Providing staff with expertise to assist the TSR development process.
- Providing institutional review of the TSR against the specifications of this procedure.

5. TECHNICAL SAFETY REQUIREMENTS DEVELOPMENT PROCESS

This procedure provides a methodical TSR development process that consists of the following:

(1) Specification of all TSR controls identified by the DSA and associated control item selection process.

(2) Determination of which type of TSR will cover each specified control.

(3) Preparation of the TSR document.

TSR development begins with compiling a list of controls identified in a given DSA that require TSR coverage. Next, decide which type of TSR (e.g., LCO, AC) to use for each control listed. Then prepare individual TSR controls and other sections of the TSR document [e.g., Use and Application, Definitions, Modes, generic LCOs and Surveillance Requirements (SRs)].

Note that the TSR should be developed with attention to operational flexibility and ease-of-use. A TSR's excessive specifications to manage operations can distort the DOE regulatory structure by diluting the emphasis intended for the most critical controls. The TSR document must fully cover items specified in the safety basis, but commitments to safety management programs will cover the majority of those items.

5.1 TSR CONTROL SPECIFICATION

The CIS process performed per AB-007 identifies the SSCs and administrative controls (specific and programmatic) that fulfill SC or SS functions. This establishes the initial list of controls requiring TSR coverage. For DSAs prepared in accordance with DOE-STD-3009-94, that list must consist of: (1) all hazard analysis TSR commitments in sections 3.3.2.3.2, *Defense in Depth*, and 3.3.2.3.3, *Worker Safety*; (2) all accident analysis TSR commitments in sections 3.4.2.X.5, *Summary of Safety-Class SSCs and TSR Controls*; and (3) for SSCs, the more detailed breakdown of the preceding two items, in sections 4.3.X.5 and 4.4.X.5 of Chapter 4, *Safety SSCs*.

The CIS process documented in the DSA should be reviewed both to identify information necessary for TSR development and to check for the proper implementation of the AB-007 specifications. Information necessary for TSR development may include:

- Specific safety functions called out.
- Implicit analytical assumptions.
- SSC interfaces and failure issues that define operability.
- Key physical parameters (e.g., temperature, pressure, or distance).
- Assumptions or parameters that define inspection requirements.

Questions raised by the CIS review as to inclusion or omission of controls should be resolved in the DSA before developing the TSR document. TSR development presumes the availability of an adequately derived control set and should not attempt to perform that function in the absence of acceptable documentation.

After verification of completeness, the initial list of TSRs and their associated information described above is augmented with other generically required administrative controls (e.g., facility management issues, staffing, or training) specified in DOE guidance.

5.2 DETERMINING THE TYPE OF TSR CONTROL

Once the items to be included in the TSRs are specified, it is necessary to determine the TSR control type appropriate for each item. The five types of TSRs are:

- Safety Limits (Section 5.2.1).
- Limiting Control Settings (Section 5.2.2).
- Limiting Conditions for Operation (Section 5.2.3).
- Administrative Controls (Section 5.2.4).
- Design Features (Section 5.2.5).

TSR preparers use their discretion, expertise, and knowledge to select the TSR control type most appropriate for the item under consideration. Once the TSR type for each relevant control is selected, Chapter 5, *Derivation of TSRs*, should be written for a DSA following the format of DOE-STD-3009-94. That chapter must accurately reflect the TSR designations specified in Chapters 3 and 4 of the DSA.

Additional guidance for selecting TSR type is provided in the following subsections.

5.2.1 Safety Limits

Safety limits (SLs) are limits on important process variables needed for the intended facility function that, if exceeded, could directly cause the failure of one or more generally passive safety class physical barriers that prevent the uncontrolled release of radioactive materials, with potential consequences to the public above specified evaluation guidelines. "Needed for the facility function," means the process variable is operator controlled to accomplish the facility mission. If left unchecked, the variable would initiate an event that challenges the passive safety boundary.

SLs are historically associated with continuous processes controlled by online parameter monitoring, which is atypical of LLNL nonreactor nuclear facility operations. If used at all, SLs are reserved for a small set of extremely significant features that prevent potentially major offsite impact. DOE-STD-3009-94 states "the majority of Hazard Category 2 facilities are not anticipated to need SLs." It further states "TSRs assigned for defense in depth and safety

significant SSCs (i.e., not related to meeting Evaluation Guidelines) will not use SLs." Accordingly, SLs should be limited in number and designated with caution; their use is not anticipated for LLNL nonreactor nuclear facilities.

5.2.2 Limiting Control Settings

Limiting control settings (LCSs) are the settings on safety systems that prevent process variables from exceeding an SL. LCSs of instruments that monitor process variables are the settings at which either protective devices actuate or alarms sound to alert facility personnel. An LCS includes specification of actions required when the limiting setting is exceeded. Assignment of an LCS also requires defining associated Surveillance Requirements that verify SSCs measuring the limiting setting and/or carrying out any associated actions are maintained.

The definition of LCS specifically associates it with SLs. Accordingly, if no SLs are assigned, there will be no LCSs.

5.2.3 Limiting Conditions for Operation

Limiting Conditions for Operation are the limits that represent the lowest functional capability or performance level of safety structures, systems, and components required for safe operations. They delineate the minimum conditions necessary to: (1) insure the initial conditions assumed in the analysis remain intact; (2) assume operability of a SSC; or (3) satisfy procedural controls. This delineation includes specific actions to be taken if those minimum conditions are not met and defines associated SRs that verify maintenance of limiting conditions and the feasibility of any associated actions.

LCOs are specifically intended to cover major active SSCs identified in the CIS process (e.g., ventilation flow providing negative pressure, fire detection and suppression, criticality alarm systems). The LCO structure defines an active capability and how it is maintained. Passive SSCs, such as a blast shield, are not normally covered by LCOs, as the associated minimum condition is simply that they exist. Such passive SSCs would typically be covered as TSR design features.

SSCs that support the safety function of another SSC may be developed as separate LCOs when that approach facilitates clarity in implementation. A common example is an emergency diesel generator providing backup electrical power to a ventilation system, a piece of equipment sufficiently complex to typically be covered by its own distinct LCO.

Note that for Hazard Category 2 facilities, DOE-STD-3009-94 states: "The decision as to whether an operating limit (such as an LCO) or a TSR administrative control is more appropriate is left to the judgment of the SAR preparer. If TSR administrative controls are used, descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why." Such guidance provides an allowance for simpler TSRs that may prove more efficient for a given application, particularly for Hazard Category 3 facilities. This procedure intentionally allows flexibility in assessing whether to assign LCOs or administrative controls; this facilitates management input regarding the set of TSRs that most effectively meets operational needs.

5.2.4 Administrative Controls

Administrative controls (AC) are selected for those provisions relating to organization and management, procedures, recordkeeping, assessment (reviews and audits), and reporting necessary to ensure safe operation of a facility. These can be broken down into three general categories: (1) specific ACs; (2) programmatic ACs; and (3) ACs for effective safety administration.

A specific AC covers a single item of sufficient importance to be called out individually. Typically, exceeding the parameters of a specific AC a single time constitutes a TSR violation. A programmatic AC commits to establish, maintain, and implement a safety management program that may have some features specifically mentioned. Programmatic discrepancies do not, however, constitute a TSR violation unless they are of sufficient quantity and magnitude to call into question the program's basic functioning. Typical programmatic ACs include radiation protection, criticality safety, fire protection, emergency preparedness, hazardous material safety, and maintenance. Inventory control is often included as well.

ACs supporting effective safety administration cover generic topics discussed in DOE G 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements*, (Ref. 6). These typically include items such as facility procedures, contractor organization and management, safety reviews and audits, record keeping, operating support, minimum staffing, facility staff qualification and training, and TSR deviations.

Active SSCs are sometimes assigned to ACs as well. This can be done for less critical SSCs when flexibility in implementation is desired or when the SSC naturally falls under an area of routine programmatic supervision. The tendency to use ACs as merely an expedient alternative to an LCO should, however, be avoided. ACs may be acceptable for ensuring safe operation, but they do not always connote the same level of reliability associated with an LCO. They can also more easily lead to TSR violations if a specific AC is used in place of an LCO with its associated action statements.

An LCO may be more appropriate and preferred for an active SSC if:

- A clear distinction between operable and inoperable is desired.
- Specific surveillances are required.
- The actions to respond to an inoperable condition must be clearly spelled out.
- What constitutes a TSR violation for an LCO is better defined than for an AC.

DOE-STD-3009-94 specifically states that for Hazard Category 3 facilities, TSRs may consist solely of an inventory limit to maintain the Hazard Category 3 classification and other ACs that provide appropriate commitments to safety programs. This minimum expectation does not apply to all circumstances, but demonstrates that a more liberal use of ACs can be acceptable for Hazard Category 3 facilities.

5.2.5 Design Features

Design features (DF) are those passive controls that, if altered or modified, would have a significant effect on safe operation. DFs are normally passive characteristics of the facility not subject to significant alteration by operations personnel (e.g., shielding, structural walls, gloveboxes, relative locations of major components, installed poisons, or special material) and which accomplish their function intrinsically as opposed to actuating in some fashion. Active safety features are subject to other TSR types (e.g., LCO, AC) and should not be included in the Design Features section.

The attributes of the passive design features that are important in the DSA should be described completely. Although specific SRs are not included in the TSRs for DFs, necessary maintenance must be addressed programmatically at a minimum.

5.3 PREPARING THE TSR DOCUMENT

Once the type of TSR control (e.g., SL, LCS, LCO, AC, or DF) is determined for each item that must be covered and Chapter 5 of the DSA, *Derivation of TSRs*, is prepared, the TSR document itself must be written. The TSR must be consistent with the designations made in Chapter 5 of the DSA, which must in turn be consistent with the designations made in Chapters 3, *Hazard and Accident* Analysis, and 4, *Safety SSCs*, of the DSA.

The front matter of the TSR document should consist of a title page, a table of contents, a list of tables, a list of figures, and a list of acronyms used. The first section of the TSR, "Use and Application," (Section 1) provides the definitions and instructions necessary to understand and use the TSR. Section 1 is placed first to provide the ground rules for use of the TSR before presenting any requirements. The next four sections of the TSR follow in hierarchical order related to the roles they have in controlling hazards. SLs (Section 2), if used, represent the most bounding control. Operating Limits (Section 3/4), which include LCSs and LCOs, protect against exceeding SLs and ensure that minimum acceptable conditions for operation are met. Section 3 numeric identifiers (e.g., 3.1.1, 3.2.1) state the operating limits, while section 4 numeric identifiers (e.g., 4.1.1, 4.2.1) state their associated SRs. They are presented together in the text of the TSR document because of their direct relationship; the combined TSR section is designated as Section 3/4. ACs (Section 5) provide assurance that the basic integrated safety management structure the safety analysis assumes is in place. Finally, the DFs (Section 6) identify and commit to maintenance of those important passive design features not amenable to description in terms of LCSs and LCOs.

Complex, Hazard Category 2 nonreactor facilities are expected to have the most extensive TSRs. The greater the hazard and complexity of a facility, the greater the number of limits and safety-related systems needed to define the bounds of operation. The scope and content of TSRs should always be limited to the most important controls, with programmatic ACs described in a brief, summary fashion. The TSR should also be written in a clear, concise manner using language that is directed at the facility-operating organization.

Additional guidance on TSR formatting and content may be found in DOE G 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements.*

5.3.1 Use and Application Section

This section should contain basic information and instructions for using and applying the information found in the TSR document. The following minimum elements must be addressed under separate headings:

- Definitions.
- Operational modes.
- Frequency notation.

While not required, the language conventions used for logical connectors and completion times are often defined.

5.3.1.1 Definitions

An alphabetical list of terms used throughout the TSR and their corresponding definitions must be provided. Include a note on the first page of the list stating that defined terms appear in uppercase type throughout the TSR (e.g., OPERATION vs. operation).

5.3.1.2 Modes

Modes must be defined for specific facility operational states based on required control capability. Maximum control capability is typically associated with the fully operating mode, with lesser capabilities required for more operationally restricted modes.

DOE has defined the following modes as general guidance:

- Operation - The mission of the facility or its current campaign is being performed.
- Startup - The facility is operating in a transient state from shutdown or near shutdown to reach conditions where the mission or campaign is performed.
- Shutdown - The facility is not performing its mission or its current campaign, and is incapable of doing so in its present condition.
- Warm Standby - The facility is not operating but still retains its inventory of hazardous material.
- Repair - The facility is not able to perform its mission in its current condition. There may also be a substantially reduced inventory.

These modes do not represent requirements. DOE provided them as examples of the operational distinctions that can be made. Facilities may choose to have fewer modes or to name and define

them differently. Modes should be established based on the minimum number needed to distinguish between desired facility conditions as dictated by required equipment operability and parameter limits (e.g., material-at-risk, fire loading). A clear line of demarcation (e.g. material handling allowed or not, material presence allowed or not, equipment functional or not) should be established between the modes to minimize the potential for TSR violation.

The "Safest Mode" is a mode in which TSR requirements do not apply. However, for nonreactor nuclear facilities it may not be possible to define a mode where some requirements do not apply as the hazard may always be present. In that case, the safest mode is that which minimizes risk.

5.3.1.3 Frequency Notation

Frequency notations used in the surveillances and elsewhere must be defined. The conventions endorsed by DOE are presented on the following page and should be used absent a compelling reason to depart from precedent. NOTE: The 25% extension to the surveillance frequency allowed by SR 4.0.2 may be added to this table to ensure consistency of application.

Notation		Minimum Frequency
S	Shiftly (i.e., each shift)	At least once every 12 hours
D	Daily	At least once every 24 hours
W	Weekly	At least once every 7 days
M	Monthly	At least once every 31 days
Q	Quarterly	At least once every 92 days
S/A	Semiannually	At least once every 184 days
A	Annually	At least once every 365 days
C	Campaign	Before startup of each campaign
S/U	Startup	Before each startup
N/A	Not applicable	Not applicable

5.3.1.4 Logical Connectors and Completion Times

Although these sections are not required, they may be beneficial to include as they cover topics that can cause confusion in TSR implementation.

The only logical connectors that appear in the TSR are "AND" and "OR." The logical connector "AND" should be used to connect two or more sets of criteria that must both (all) be satisfied for a given logical decision. If more than two sets of conditions are required, a list format is preferable. The logical connector "OR" should be used to denote alternative combinations or conditions, meaning either one or the other.

Completion time conventions cover such issues as the point at which time measurement begins, the point at which it ceases, the relationships between multiple completion times for multiple actions, or nested completion times (i.e., an inoperable condition discovered while in the completion time for another inoperable condition). Completion times also define the intended meaning of qualitative phrases such as "immediately."

5.3.2 Preparation of Safety Limits

The safety limit section of the TSR (Section 2) describes, as precisely as possible, the parameters being limited and indicates the applicability of the limit. The safety limit section also describes the actions to be taken if the safety limit is exceeded. As a minimum, each individual SL must contain an SL statement, a mode applicability statement, and action statements. These entries are discussed further in Section 5.3.3.4, *Preparation of Limiting Conditions for Operation*, where they are most applicable for LLNL facilities. The SL does not have SRs, as these would be associated with a LCS that protects the SL.

Exceeding a SL is a TSR violation for each applicable mode. Upon exceeding a SL, the following steps should be taken:

- The affected parameter must be immediately brought within the SL.
- The facility must be placed in the most stable, safe condition attainable, including shutdown if appropriate.
- All other ACTION requirements should be met.

A statement prohibiting restart, before DOE approval, of the facility (or operation, depending on the most stable, safe facility condition) after an SL violation should be included in the ACTION statement of each SL, in Section 5 (Administrative Controls) of the TSR, or in both.

5.3.3 Preparation of Operating Limits

The operating limit (OL) section of the TSR (Section 3/4) contains LCSs, LCOs, and their associated SRs. Section 3.0 defines generic LCOs. Section 4.0 follows immediately thereafter and defines generic SRs. Sections 3.1 and 4.1 then define the first LCS/LCO followed by its specific SRs, and so on until all LCSs/LCOs and their SRs are defined.

This section of the procedure defines operability and generic LCOs/ SRs and provides guidance on preparing LCSs, LCOs and SRs.

5.3.3.1 Operability

Operability embodies the principle that a system, subsystem, train, component, or device (hereafter referred to as the system) can perform its safety functions only if all necessary support systems are capable of performing their support functions. This definition extends the

requirements of an LCO for those systems that directly perform a specified safety function (supported systems) to those that perform a required support function (support systems).

A system or component can be degraded but still be operable if it remains capable of performing its required safety function at the level assumed in the DSA. If systems, components, or equipment are observed to be functioning but under stress (e.g., with elevated temperature, vibration, or physical damage), then judgment must be used concerning a declaration of inoperability.

The following general principles of operability should be followed when generating LCOs:

1. A system is considered operable as long as there exists assurance that it is capable of performing its specified safety functions.

2. A system can perform its specified safety functions only when all of its necessary support systems are capable of performing their related support functions.

3. When all systems designed to perform a certain safety function are not capable of performing that safety function, a loss of function condition exists.

4. When a system is determined to be incapable of performing its intended safety functions, the declaration of inoperability should be immediate.

These general principles of operability are not included in the TSR as a separate section. However, a definition for operable/operability that addresses these concepts should be included in the definitions section of the TSR.

5.3.3.2 Generic LCOs and SRS

Generic LCOs and SRs provide the framework within which the specific LCOs and SRs operate. They set the limitations and general parameters that should be followed and considered when developing specific LCOs. The generic LCOs and SRs do not apply to the Administrative Controls section of the TSR document.

The wording for the Generic LCOs and SRs is standardized. This wording should be used when facility-specific terminology and conditions can clarify standard language. The generic LCOs of concern are:

LCO 3.0.1 *LCOs must be met during the MODES specified in the Applicability, except as provided in LCO 3.0.2. Completion of the required ACTIONS for the MODE is considered to be in compliance with the applicability of the MODE.*

This establishes the basic requirement to meet LCOs as they are defined.

LCO 3.0.2 *Upon discovery of a failure to meet an LCO, the associated ACTIONS must be met. If the LCO is restored before the specified COMPLETION TIME(S) expires, completion of the ACTION is not required, unless otherwise stated.*

This establishes the basic requirement to implement LCO Action statements when LCOs are not met.

LCO 3.0.3 *When an LCO is not met and the associated ACTIONS are not met, or when an associated ACTION is not provided, the facility shall be placed in a MODE or other specified condition in which the LCO is not applicable. If the LCO is applicable in all MODES, the facility shall be placed in the safest MODE. Activities shall be initiated to place the affected PROCESS AREA(S) or the facility in STANDBY (or the safest mode) within 1 hour. The affected PROCESS AREA or facility shall be in STANDBY (or the safest mode) within 12 hours.*

Where corrective measures are completed that permit operation in accordance with the LCO or ACTIONS, completion of the ACTIONS required by LCO 3.03 are not required.

LCO 3.0.3 is applicable in all MODES. Exceptions to LCO 3.0.3 may be stated in the individual LCOs.

This is sometimes called the "default action" LCO. It is intended to insure that required actions cover all situations threatening facility safety even if TSR document does not directly address the circumstance of concern. This generic LCO should be customized for the specific facility application to identify the facility mode names for the safest modes. The time frames to be in the safest mode (e.g., Standby) may also be modified based on the facility specific safety analysis. Exceptions are included at the discretion of the TSR preparer.

Entering LCO 3.0.3 is not considered a TSR violation if: (1) no exceptions have been taken to entering LCO 3.0.3 in the LCO causing entry into 3.0.3; (2) LCO 3.0.3 has been entered prior to expiration of the relevant completion times for the LCO causing entry into 3.0.3; and (3) all required actions of 3.0.3 are completed within their prescribed time limits (unless the LCO causing entry into 3.0.3 is successfully restored).

LCO 3.0.4 *When an LCO is not met, a MODE or other specified condition in the Applicability shall not be entered, except where the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time. LCO 3.0.4 does not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with ACTIONS.*

Exceptions to LCO 3.0.4 are stated in the individual LCOs. When an individual LCO states that LCO 3.0.4 does not apply, it allows entry into MODES or other specified conditions in the Applicability when the Associated ACTIONS to be entered permit operation in the MODE or other specified condition for only a limited time.

This establishes mode integrity; one cannot enter a mode unless all the LCOs required for that mode are met without reliance on action statements. However mode changes are allowed when dictated by an action statement.

This LCO is typically shortened by omitting the "other specified condition" phrase and by writing to the facility-specific modes and their intended use. Exceptions are included at the discretion of the TSR preparer, provided they satisfy the criteria in the second paragraph of LCO 3.0.4.

LCO 3.0.5 *Equipment removed from service or declared inoperable to comply with ACTIONS may be returned to service under administrative control solely to perform testing required to demonstrate its OPERABILITY or the OPERABILITY of other equipment. This is an exception to LCO 3.0.2 for the system returned to service under administrative control to perform the testing required to demonstrate OPERABILITY.*

This addresses "return to service" issues by allowing testing for operability without needlessly complicating formal application of an LCO.

LCO 3.0.6 *When a support system is declared to be inoperable, the supported systems are also declared to be inoperable. However, only the support system's ACTIONS are required to be entered, provided they reflect the supported system's degraded safety condition. This is a clarification of the definition of OPERABILITY.*

This allows for the flexibility to address supporting systems on an individual basis. If a TSR does not have support system LCOs and relies on the definition of operable/operability to address any support functions, LCO 3.0.6 would not be included in the TSR.

The generic SRs of concern are:

SR 4.0.1 *SURVEILLANCE REQUIREMENTS must be met during the Operational Modes or other conditions specified for individual LCS and LCOs unless otherwise stated in an individual SURVEILLANCE REQUIREMENT.*

This establishes the basic requirement to meet SRs as they are defined, and thus the corollary that failure to meet an SR constitutes failure to meet the associated LCS or LCO. The phrase "the Operational Modes or other conditions specified" is often replaced with the phrase "the MODES specified in the Applicability." This SR is also often augmented with the following sentence: "Surveillances do not have to be performed on inoperable equipment or variables outside specified limits." The purpose of that sentence is to formally remove the SR requirement during periods of known operational failure.

SR 4.0.2 *Each SURVEILLANCE REQUIREMENT shall be performed within the specified frequency. The specified frequency for each SR is met if the surveillance is performed within 1.25 times the interval specified in the frequency as measured from the previous performance or as measured from the time a specified condition of the frequency is met.*

This SR is a combination of two SRs in DOE G 423.1-1. It establishes the basic requirement to comply with SR frequencies while formally defining the maximum frequency extension allowed for unforeseen circumstances.

SR 4.0.3 *If it is discovered that a surveillance was not performed within its specified frequency, compliance with the requirement to declare the LCO not met may be delayed from the time of discovery up to 24 hours, or up to the limit of the specified frequency, whichever is less. This delay period is permitted to allow performance of the surveillance.*

If the surveillance is not performed within the delay period, or if it is performed and the surveillance is not met, the LCO shall IMMEDIATELY be declared not met, and the applicable ACTIONS shall be entered. The COMPLETION TIMES of the ACTIONS begin IMMEDIATELY on failure to meet the surveillance.

This is sometimes called the "grace period" SR. It is intended to cover those situations where the surveillance has not been met inadvertently but the control in question is believed to remain operable. The grace period SR allows a facility to establish operability by performing the surveillance, thus negating potential mode changes that would needlessly put the facility through a major evolution in accordance with ACTION statements. However the situation must still be reported as a TSR violation.

SR 4.0.4 *Entry into an Operational Mode or other specified condition shall not be made unless the SURVEILLANCE REQUIREMENT(S) associated with the LIMITING CONDITION FOR OPERATION has been performed within the stated surveillance interval or as otherwise specified.*

This SR is the complement SR to LCO 3.0.4 in establishing the integrity of modes. If one cannot enter a mode unless all the LCOs required for that mode are met without reliance on action statements, one likewise cannot enter a mode unless the LCO's surveillances are met. However mode changes are still allowed when dictated by an action statement.

5.3.3.3 Preparation of Limiting Control Settings

The LCSs section contains the settings for variables associated with safety limits. These settings are normally associated with alarms or the initiation of protective actions. This section also identifies the protective actions to be taken at the specific settings chosen to correct a situation automatically or manually such that the related safety limit is not exceeded. Protective actions may include maintaining the variables within the requirements and repairing the automatic device promptly or shutting down the affected part of the process and, if required, the entire facility. As a minimum, each individual LCS must contain a LCS statement, a mode applicability statement, action statements, and SRs.

LCSs should encompass, at a minimum, three basic rules:

1. Compliance with an LCS is required in the modes specified.

2. Upon discovery that the instrumentation or interlock set point is less conservative than the required LCSs, the associated ACTION should require that it be reset. Other actions should be specified (e.g., the time allowed out of service for resetting, test, maintenance, repair, or calibration).

3. If an automatic safety system is not OPERABLE as specified, the ACTION statement should describe the appropriate action to compensate. In nonreactor nuclear facilities, such action might be manual process shutdown/process adjustment or engineered safety feature initiation/adjustment.

The LCS, or an associated LCO, should specify the allowed out-of-service time permitted when testing, resetting, repairing, or maintaining trip devices and similarly the time permitted for associated equipment that must be removed from service for these activities.

As LCOs are the typical operating limit for nonreactor nuclear facilities, general guidelines for operating limit statements, mode applicability statements, and action statements are discussed under section 5.3.3.4, *Preparation of Limiting Conditions for Operation.*

5.3.3.4 Preparation of Limiting Conditions for Operation

The LCOs section describes, as precisely as possible, the lowest functional capability or performance level of equipment required for continued safe operation of the facility. The LCO section also identifies the corrective or compensatory actions to be taken to either restore compliance with the LCO statement or to monitor the control covered by the LCO statement while allowing time to restore the inoperable SSC or parameter. Protective actions may include maintaining the variables within the requirements and repairing the inoperable equipment or shutting down the affected part of the process and, if required, the entire facility. As a minimum, each individual LCO will contain an LCO statement, mode applicability statement, action statements, and SRs. Note that when support and supported systems are in separate LCOs, these must be developed so as not to contradict one another.

LCOs should encompass, at a minimum, three basic rules:

1. Compliance with an LCO is required in the modes specified.

2. The LCO should include an allowable outage time to attempt restoration of the required functional performance (operability).

3. Upon failure to meet an LCO, the associated ACTION requirement should be met.

LCS/LCO Statement

LCS/LCO specification statements should be concise. The objective is to distill a clear, precise statement or specification of operability. This includes a statement that the "X" system must be operable in conjunction with whatever SSCs or parameter specifications are deemed to require specific mention. For example, "The criticality alarm system must be OPERABLE with two detection channels and an alarm set point for each detector set at less than or equal to 100 mR/hr." Or, "the exhaust ventilation system shall be OPERABLE with two exhaust fans maintaining flow greater than or equal to 2,500 cfm and two HEPA filter banks each with a removal efficiency greater than or equal to 99.9% for 0.3 micron particles or greater." The LCS/LCO specification statement typically focuses on the most important SSCs and parameters, and is not required to individually list all subcomponents. The complete list is detailed in the SRs

demonstrating compliance with the LCO statement, except where key support SSCs have been assigned their own individual LCO.

The LCS/LCO specification statement must be kept distinct from other components of the LCS/LCO. Including mode applicability issues, surveillance requirements, and external document references in the specification statement is a common error. At best, this yields an awkward LCO. At worst, it creates systemic logic flaws that inevitably yield TSR violations upon implementation. The specification statement is the top-level definition that flows down into other components of the LCS/LCO.

Note that the phrases "OPERABLE and operating" or "OPERABLE and in standby" are not necessary. The definition of OPERABLE means the equipment is performing its intended function, which may be in service or in standby.

Applicability Statement

A mode applicability statement must be included for each LCS/LCO. This statement should consist of a simple listing of the modes for which the LCS/LCO is applicable. When a given LCO applies only to specific locations or process areas, a location applicability statement should also be included. This would consist of a simple listing of relevant areas immediately following the mode applicability statement.

Modifying the mode applicability to limit the scope of LCS/LCO applicability to a condition/situation that is a subset of the defined mode is sometimes necessary. The applicable modes are listed followed by text that modifies the applicability. For example, "OPERATION, when the vault door is open and fissile material is present." A simple modifier can be applied to a single condition or the entire applicability statement. If a modifier only applies to one Mode, list the Mode being modified on a separate line from the Modes not being modified.

Action Statements

Action statements describe: (1) the specific operating limit issue that requires a response (Condition Statement); (2) the response to be made (Required Action); and (3) the allowable time in which to perform that response (Completion Time). Action statements should be written in direct, simple language focused on clarity, action verbs (e.g., verify, restore, perform), and single, distinct statements.

The condition statement states: (1) a given set point exceedance for LCSs, (2) a given inoperable configuration for LCOs, or (3) that the action and associated completion time for a given inoperable condition has not been met. The first two conditions cover direct entry into TSR Actions; the third condition covers sequential steps that must be taken after entry into TSR Actions. Condition statements should be written for every set point exceedance and foreseeable inoperable configuration that is not a trivial variant of another inoperable configuration. General condition statements can also be used. For example: "The Room Ventilation System is inoperable for reasons other than those specified in Conditions A, B, C, and F." Such general

condition statements are only acceptable, however, if a general required action is readily applicable.

A required action provides a safe and unambiguous method to reach a safe and stable state. That state may be reached by a given action statement itself, or by a sequential action statement predicated on failure to meet its preceding action statement. An example would be a given action statement to restore ventilation flow within three hours and the sequential action statement that if flow is not restored within that time, the required action is to shift operating status to a different mode.

Two basic types of required actions exist: corrective or compensatory. The corrective required action restores the inoperable equipment within the time allowed or places the facility in a Mode where the LCO does not apply and the control is not required. The compensatory required action designates another piece of equipment or control (e.g., alternate equipment or monitoring activity) that can temporarily provide the safety function required by the original inoperable equipment.

Completion times are typically discrete time periods (e.g., 24 hours or 7 days) in which the required action must be accomplished. However, some required actions (particularly compensatory measures) may have to continue to be performed periodically. In such cases, the completion time includes an initial performance followed by subsequent periodic performances (e.g., 24 hours and every 7 days thereafter). Completion times are referenced to time of discovery of a condition. When in multiple conditions, separate completion times are tracked for each condition starting from the discovery time of the situation requiring entry into a given condition.

In general, the more serious a safety degradation, the shorter the associated completion time should be. Completion times are based on factors such as estimated time to reach a condition of concern (e.g., lower flammable limit in a process tank's air space), actual completion time for a well-defined repair task, operating experience, risk or failure rate data (if available), or available redundancy. Any or all of these factors require some degree of engineering judgment.

5.3.3.5 Preparation of Surveillance Requirements

SRs specify the requirements relating to test, calibration, or inspection necessary to ensure that the associated LCS/LCO is met. These requirements must cover all SSCs and conditions stated in the LCS/LCO statement. The surveillance requirements section (Section 4 of the TSR) consists of a surveillance statement and the associated frequency.

Surveillance Requirement Statements

SR statements consist of short definitions of the type of surveillance required to ensure compliance with the associated LCS/LCO. For example, "Verify that the pressure in Room 27A is a minimum of 0.05 inch WG lower than the outside atmospheric pressure by checking the wall-mounted differential pressure gage." Or, "Perform a channel functional test on each criticality alarm system detector using an external radiation source." The total collection of SR statements associated with a given LCS/LCO should: (1) confirm operability of any required

safety equipment; (2) maintain facility operations within LCS/LCO; and (3) detect unidentified failures or potential failures. Operability of equipment is confirmed by full load testing, functional testing, or calibrating equipment.

Surveillance Requirement Frequencies

SR frequencies are direct statements of the time interval in which the surveillance must be performed. One-word statements (e.g., weekly, monthly, quarterly, annually) are preferred. The interval can be based on specific DSA assumptions, national and international codes, standards, and guides, reliability analyses, failure modes and effects analyses, manufacturer documentation, information from operating history, or engineering judgment.

SR 4.0.2 in the Generic LCO/SR section does allow a 25% extension to the SR interval, which should be considered when establishing the SR frequency. If this extension would invalidate an analytical assumption, a note may need to be added stating SR 4.0.2 extension is not allowed or does not apply to a particular SR.

5.3.4 Preparation of Administrative Controls

The AC section (Section 5 of the TSR) formally defines the administrative requirements necessary to provide safe operation of the facility. As previously noted in section 5.2.4, *Administrative Controls*, this section defines three general categories of ACs: (1) specific ACs; (2) programmatic ACs; and (3) ACs for effective safety administration.

5.3.4.1 Specific Administrative Controls

Specific ACs state a specific administrative requirement that will be met when operating. For example, "TRU waste containers shall not be stacked more than two levels high, and the bottom of the second level shall be stored no more than nominally 4 feet above ground." A separate specific AC should be developed for each distinct administrative requirement.

Use of specific ACs is not required, but is an option when facility management and DOE concur that an administrative requirement is of sufficient importance to be singled out but not included in an LCO. Typically, a single violation of a specific AC constitutes a TSR violation. However, with DOE's concurrence, specific ACs can be phrased to limit that potential. For example, "All TRU waste drums stored on the second level shall be banded together per pallet upon initial placement. Damaged bands shall be replaced upon discovery." This simple example allows the deviation if it is corrected upon discovery.

5.3.4.2 Programmatic Administrative Controls

Programmatic ACs commit to a safety management program that will oversee day-to-day activities. Programmatic ACs typically begin with the phrase "A _____ program shall be established, implemented, and maintained to ensure that…" For example:

A radiation protection program shall be established, implemented, and maintained to ensure that radiation exposure to employees, subcontractors, visitors, and members of the general public is controlled in accordance with requirements of 10 CFR 835, as implemented in the *ES&H Manual* Document 20.5.

Some programmatic ACs highlight major aspects of the program in bullet fashion. For example:

A fire protection program shall be established, implemented, and maintained to minimize the likelihood of fire in accordance with all contractor-applicable provisions of DOE Order 420.1A, as implemented in *ES&H Manual* Document 22.5. Key provisions of this program include:

- a safety significant fire suppression system;
- maximum room fuel loading of 10 kg/m^2 as verified by periodic inspections;
- allowance for only incidental quantities of flammable or combustible liquids in three appropriate storage cabinets; and
- use of non-combustible storage racks in glovebox processing lines 5, 8, and 12.

Specifying key elements does not make those elements specific ACs. They remain under the control of a programmatic AC, which require cumulative violations of sufficient quantity and magnitude that call into question basic implementation to constitute a TSR violation.

5.3.4.3 ACs for Effective Safety Administration

DOE guidance has historically identified a number of ACs generically. These are both holdovers from traditional U.S. Nuclear Regulatory Commission practice and some programmatic ACs of heightened interest. Even if these items do not specifically derive from the DSA, they should be included in the TSR document.

A brief summary follows:

1. Contractor Responsibility. States that the facility or plant manager is responsible for overall operation of the nuclear facility, summarized as appropriate, and should delegate in writing the succession to this responsibility during his or her absence.

2. Contractor Organization. Summarizes the organizations responsible for maintaining the safety basis in terms of lines of authority, responsibility, and communication.

3. Minimum Operations Shift Complement. Includes the required staffing of operating shifts by position and normal working hours.

4. Operating Support. Provides a commitment to maintain a referenced list of facility support personnel by name, title, and work and home telephone numbers.

5. Facility Staff Qualifications and Training. Provides a statement as to minimum qualifications for members of the facility staff in positions affecting safety (conforming to requirements of DOE 5480.20A or successor document).

6. Procedures. Provides a commitment to develop appropriate procedures to maintain the safety basis and to implement proper change control practices for such procedures.

7. Record Keeping. Provides a commitment to collect and maintain all information supporting the safety basis, including operational logs of modes changes, entering actions, surveillances, deviations, procedures, programs, meetings, recommendations, etc.

8. Reviews and Audits. Provides a commitment to conduct facility staff reviews or independent reviews and audits.

9. Deviations from Technical Safety Requirements. States the actions and reporting to be taken for deviations from TSRs. This should include the person (or position) in authority, as designated in the TSRs, to approve "emergency actions that depart from an approved technical safety requirement when no actions consistent with the technical safety requirement are immediately apparent, and when these actions are needed to protect workers, the public or the environment from imminent and significant harm. (10 CFR 830.205 (b))."

5.3.5 Preparation of Design Features

The DF section (Section 6 of the TSR) provides a commitment to maintain as described those passive features not captured elsewhere in the TSRs that, if altered or modified, would have a significant effect on safety. The following two areas should be addressed in this section:

1. Vital passive safety SSCs such as piping, vessels, supports, structures (e.g., confinement), and containers.

2. Configuration or physical arrangement including dimensions, the parameters being controlled, and the reasoning behind the design should be provided as identified in the safety analysis. Examples include situations in which criticality avoidance is dependent on physical separation features or equipment configuration is used to minimize radiation levels.

The important assumptions regarding these passive DFs, as determined by the DSA, should be described completely. Although specific SRs are not included in the TSRs for DFs, any necessary surveillances are typically addressed programmatically through such programs as configuration management or in-service inspections.

5.3.6 Preparation of Bases

The TSR bases appendix (Appendix A of the TSRs) provides summary statements explaining why each SL, LCS/LCO, and associated SRs are specified as written. ACs do not require bases.

The bases detail specifics how the numerical values, conditions, surveillances, and action statements fulfill the purpose of maintaining the safety basis. These specifications provide necessary background material to assist in interpreting the main TSR document's summary statements. The bases appendix should summarize and reference any more specific analyses related to the TSRs and their derivation.

The content of the bases appendix is divided into seven areas: background, application to safety analysis, SLs and OLs, mode applicability, ACTION statements, SRs, and references:

1. Background. Defines each relevant SSC or control in terms of general design, multiple SSC relationships, operational aspects, and unique features. The description should be sufficiently detailed for operations personnel to confirm the definition of OPERABLE.

2. Application to Safety Analysis. Defines the DSA assumptions a given SL or LCS/LCO is intended to protect, in terms of hazards and accidents, documented consequences, and margin of safety, if applicable.

3. SL or OL. Explains why the requirement is appropriate (i.e., why is it an acceptable functional capability or performance level?), matching the DSA assumptions protected to specific conditions of the SL or OL.

4. Mode Applicability. Presents information on expected operational conditions (e.g., start-up, operation, shutdown) that establish sufficient unique or distinguishing characteristics to permit understanding and acceptance of the TSR modes as stated for the given SL or OL. (NOTE: A location applicability section should also be presented if location applicability was assigned in the associated SL or OL.)

5. Action Statements. Explains justification of the action, the given level of continued operation if the LCO is not met, and the completion time. This discussion is typically phrased in terms of the source of all numbers, the level of protection provided, the probability of an event occurring during the period covered, and how the required actions compensate for LCO deviations.

6. Surveillance Requirements. Explains why the surveillance demonstrates operability at the frequency specified. This discussion is typically phrased in terms of the source of all numbers, an exact description of what constitutes the surveillance, what is specifically tested, and what the testing demonstrates.

7. References. Identifies a list of documents that contain more detailed information pertinent to the specification, in terms of DSA sections, reports, and codes and standards, as applicable.

Note that when developing TSR limiting values or set points based on the DSA, the values in the DSA are generally the exact values at which something is assumed to happen. Because the values and set points in the TSR are measured, the DSA values must be adjusted before use in the TSR to ensure that the action assumed in the DSA actually occurs on the conservative side of the DSA assumptions. The adjustments should account for: calibration uncertainty, instrumentation uncertainty during operation, instrument drift, and instrument uncertainty during accident conditions.

6. REFERENCES

1. *Preparation Guide for U.S. Department of Energy Non-Reactor Nuclear Facility Safety Analysis*. DOE-STD-3009-94, Change Notice #1, U.S. Department of Energy, Washington, DC, January 2000.

2. *Nuclear Safety Management*. 10 CFR Part 830, U.S. Department of Energy, Washington, DC.

3. *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans*. DOE-STD-3011-94, U.S. Department of Energy, Washington, DC, November 1994.

4. *Safety Basis Program Plan for Hazard Category 2 and 3 Nuclear Facilities*. AB-001, Lawrence Livermore National Laboratory, Livermore, CA, August 2001.

5. *Control Item Selection procedure for Hazard Category 2 and 3 Nuclear Facilities*. AB-007, Lawrence Livermore National Laboratory, Livermore, CA, October 2002.

6. *Implementation Guide for Use In Developing Technical Safety Requirements*. DOE G 423.1-1, U.S Department of Energy, Washington D.C., October 2001.

This page intentionally left blank.